

RECEIVED  
CENTRAL FAX CENTER

DEC 19 2006

**Listing of Claims:**

This listing of claims will replace all prior versions, and listings, of claims in the application. This listing of the claims presumes that the amendments made in the Amendment mailed on December 4, 2006, have already been entered.

1. - 8. (Canceled).

9. - 16. (Canceled).

17. - 154. (Canceled).

**155. (Currently amended)** A method for verifying whether an e-mail sent by a sending party was accessed by an intended recipient, said method comprising:

a) storing recipient data pertaining to an actual recipient of e-mail in a data file, said stored data file containing identifying data that identifies said actual e-mail recipient and further being associated with said actual recipient's email address;

b) transmitting an e-mail from a sender computer to an intended recipient, the sender computer being connected to a communications network;

c) delivering said e-mail to an a recipient e-mail address;

d) detecting an access event, and discovering said stored data file that is associated with said actual recipient's e-mail address; and

e) sending identifying data contained in said discovered data file for confirming proper delivery of said e-mail.

1 **156. Canceled.**

2  
3 **157. (Previously presented)** The method as in claim 155, wherein said access event  
4 comprises access of said e-mail that was delivered to said actual recipient e-mail address.

5  
6 **158. (Previously presented)** The method as in claim 155, wherein said access event comprises  
7 access of an email account associated with said actual recipient e-mail address.

8  
9 **159. (Previously presented)** The method as in claim 155, wherein said access event comprises  
10 activation of an e-mail processing software associated with said actual recipient e-mail address.

11  
12 **160. (Previously presented)** The method as in claim 155, wherein the step of transmitting an  
13 e-mail from a sender computer includes attaching an executable attachment file in conjunction with  
14 the e-mail, the executable attachment file having a first module for discovering the stored data file  
15 that is associated with said actual recipient's email address and wherein the step of detecting an  
16 access event includes the step of executing the first module of the executable attachment file.

17  
18 **161. (Previously presented)** The method as in claim 160, wherein the executable  
19 attachment file has a second module transmitted and delivered therewith, the second module for  
20 detecting the access event, and

21 further comprising the step of:

22 automatically executing the second module upon delivery of the attachment file to the  
23 actual recipient e-mail address.

24  
25 **162. Canceled.**

1 163. (Currently amended) The method as in claim 155, wherein said actual recipient email  
2 address is associated with ~~an actual~~ a recipient computer.

3  
4 164. (Currently amended) The method as in claim 163, wherein said ~~actual~~ recipient computer  
5 is a server of a service provider.

6  
7 165. (Currently amended) The method as in claim 163, wherein said ~~actual~~ recipient computer  
8 is a user system that is directly accessible by the actual recipient, said user system including  
9 electronic mail processing software.

10  
11 166. (Previously presented) The method as in claim 155, wherein a remote user computer may  
12 be used to gain remote access to said actual recipient e-mail address.

13  
14 167. (Previously presented) The method as in claim 155, wherein said identifying data  
15 contained in said stored data file pertains to alphanumeric text identification, biometric  
16 identification, password identification, a computer generated user code, or a combination thereof.

17  
18 168. (Previously presented) The method as in claim 155, wherein said stored data file  
19 comprises identity information that identifies an individual.

20  
21 169. (Previously presented) The method as in claim 168, wherein said identity  
22 information pertains to biometric identification.

23  
24 170. (Previously presented) The method as in claim 169 further comprising the step of  
25 recognizing biometric attributes of an individual.

26  
27

1  
2 **171. (Previously presented)** The method as in claim 168, wherein said identity information  
3 includes alphanumeric text identification information.

4  
5 **172. (Previously presented)** The method as in claim 155, wherein said stored data file  
6 comprises information that identifies a business.

7  
8 **173. (Previously presented)** The method as in claim 155, wherein said stored data file  
9 comprises information that identifies an organization.

10  
11 **174. (Previously presented)** The method as in claim 155, wherein said stored data file  
12 comprises a computer generated user code.

13  
14 **175. (Previously presented)** The method as in claim 155 further including the step of sending  
15 access event data of conditions attendant said access event.

16  
17 **176. (Previously presented)** The method as in claim 155, wherein said actual recipient is  
18 an individual.

19  
20 **177. (Previously presented)** The method as in claim 155, wherein said actual recipient is a  
21 business.

22  
23 **178. (Previously presented)** The method as in claim 155, wherein said actual recipient is  
24 an organization.

1 **179. (Previously presented)** The method as in claim 155, wherein said step of sending  
2 identifying data is used to verify proper delivery of legal documents.

3  
4 **180. (Previously presented)** The method as in claim 155, wherein said step of sending  
5 identifying data is used to verify proper delivery of confidential documents.

6  
7 **181. (Previously presented)** The method as in claim 155, wherein said data file is stored  
8 on a computer associated with e-mail retrieval.

9  
10 **182. (Previously presented)** The method as in claim 155, wherein said identifying data for  
11 confirming proper delivery of said e-mail is sent to an e-mail address.

12  
13 **183. Canceled.**

14  
15 **184. (Currently amended)** The method as recited in claim 258 wherein said step of sending  
16 recipient data for confirming proper delivery of said e-mail includes the steps of:

17 a) generating a confirmation of receipt notice wherein the inputted recipient data is  
18 included with said confirmation of receipt notice; and

19 b) sending said confirmation of receipt notice, wherein the inputted recipient data included  
20 with said confirmation of receipt notice can be compared to ~~delivery~~ information associated with  
21 said intended recipient in order to verify whether the email e-mail was accessed by the intended  
22 recipient.

23  
24 **185. (Previously presented)** The method as in claim 236, wherein said access event  
25 comprises access of said e-mail that was delivered to said recipient e-mail address.

1 **186. (Currently amended)** The method as in claim 236, wherein said access event  
2 comprises access of an ~~email~~ e-mail account associated with said recipient e-mail address.

3  
4 **187. (Previously presented)** The method as in claim 236, wherein said access event  
5 comprises activation of an e-mail processing software associated with said recipient e-mail address.

6  
7 **188. (Currently amended)** The method as in claim 236, ~~further comprising the steps of:~~  
8 wherein the step of transmitting an e-mail from a sender computer includes attaching  
9 ~~transmitting and delivering to the recipient e-mail address an executable attachment file in~~  
10 ~~conjunction with the e-mail, the executable attachment file having a first module for prompting the~~  
11 ~~party who requested said access event to enter recipient data, a second module for generating the~~  
12 ~~confirmation of receipt notice, and a third module for transmitting the confirmation of receipt~~  
13 ~~notice; and~~  
14 ~~upon the detection of the access event, automatically executing the first, second, and third~~  
15 modules and wherein the step of detecting an access event includes the step of executing the first  
16 module of the executable attachment file.

17  
18 **189. (Currently amended)** The method as in claim 188, wherein the executable  
19 attachment file has a fourth second module transmitted and delivered therewith, the fourth second  
20 module for detecting the access event, and further comprising the step of automatically executing  
21 the fourth second module upon delivery of the attachment file to the recipient e-mail address.

22  
23 **190. Canceled.**

24  
25 **191. (Previously presented)** The method as in claim 236, wherein said recipient e-mail  
26 address is associated with a recipient computer.

1 **192. (Previously presented)** The method as in claim 191, wherein said recipient computer  
2 is a server of a service provider.

3  
4 **193. (Previously presented)** The method as in claim 191, wherein said recipient computer  
5 is a user system that is directly accessible by a recipient, said user system including electronic mail  
6 processing software.

7  
8 **194. (Previously presented)** The method as in claim 236, wherein said inputted recipient  
9 data pertains to alphanumeric text identification, biometric identification, password identification, a  
10 computer generated user code, or a combination thereof.

11  
12 **195. (Previously presented)** The method as in claim 236, wherein said inputted recipient  
13 data comprises identity information that identifies an individual.

14  
15 **196. (Previously presented)** The method as in claim 195, wherein said identity  
16 information pertains to biometric identification.

17  
18 **197. (Currently amended)** The method as in claim 196 further comprising ~~means for the~~  
19 step of recognizing biometric attributes of an individual.

20  
21 **198. (Previously presented)** The method as in claim 195, wherein said identity  
22 information includes alphanumeric text identification information.

23  
24 **199. (Previously presented)** The method as in claim 236, wherein said inputted recipient  
25 data comprises information that identifies a business.

1 **200. (Previously presented)** The method as in claim 236, wherein said inputted recipient  
2 data comprises information that identifies an organization.

3  
4 **201. (Previously presented)** The method as in claim 236, wherein said inputted recipient  
5 data comprises a computer generated user code.

6  
7 **202. (Previously presented)** The method as in claim 236 further including the step of  
8 sending access event data of attendant conditions of said access event.

9  
10 **203. (Previously presented)** The method as in claim 236, wherein said recipient is an  
11 individual.

12  
13 **204. (Previously presented)** The method as in claim 236, wherein said recipient is a  
14 business.

15  
16 **205. (Previously presented)** The method as in claim 236, wherein said recipient is an  
17 organization.

18  
19 **206. (Previously presented)** The method as in claim 236, wherein said inputted recipient  
20 data is used to verify proper delivery of legal documents.

21  
22 **207. (Previously presented)** The method as in claim 236, wherein said inputted recipient  
23 data is used to verify proper delivery of confidential documents.

24  
25 **208. (Currently amended)** The method recited by claim 260 wherein said step of sending  
26 recipient data for confirming proper delivery of said e-mail includes the steps of:  
27



1 a) generating a confirmation of receipt notice wherein the acquired recipient data is  
2 included with said confirmation of receipt notice; and

3 b) sending said confirmation of receipt notice, wherein the acquired recipient data  
4 contained with said confirmation of receipt notice can be compared to ~~delivery~~ information  
5 associated with said intended recipient in order to verify whether the email was accessed by the  
6 intended recipient.

7  
8 **209. (Previously presented)** The method as in claim 260, wherein said access event  
9 comprises access of said e-mail that was delivered to said recipient e-mail address.

10  
11 **210. (Currently amended)** The method as in claim 260, wherein said access event  
12 comprises access of an ~~email~~ e-mail account associated with said recipient e-mail address.

13  
14 **211. (Previously presented)** The method as in claim 260, wherein said access event  
15 comprises activation of e-mail processing software associated with said recipient e-mail address.

16  
17 **212. (Currently amended)** The method as in claim 260, ~~further comprising the step of:~~  
18 wherein the step of transmitting an e-mail from a sender computer includes attaching  
19 ~~transmitting and delivering to the recipient e-mail address~~ an executable attachment file in  
20 conjunction with the e-mail file, the executable attachment file having a first module for acquiring  
21 recipient data that is related to biometric identification of the recipient, ~~a second module for~~  
22 ~~generating the confirmation of receipt notice, and a third module for transmitting the confirmation~~  
23 ~~of receipt notice; and~~

24 ~~upon the detection of the access event, automatically~~ wherein the step of detecting an access  
25 event includes the step of executing at least the second and third modules first module of the  
26 executable attachment file.  
27

1 **213. (Currently amended)** The method as in claim 212, wherein the executable  
2 attachment file has a ~~fourth~~ second module transmitted and delivered therewith, the ~~fourth~~ second  
3 module for detecting the access event, and further comprising the step of:  
4 automatically executing the ~~fourth~~ second module upon delivery of the attachment file to  
5 the recipient e-mail address.

6  
7 **214. Canceled.**

8  
9 **215. (Previously presented)** The method as in claim 260, wherein said recipient e-mail  
10 address is associated with a recipient computer.

11  
12 **216. (Previously presented)** The method as in claim 215, wherein said recipient computer  
13 is a server of a service provider that is capable of receiving e-mail.

14  
15 **217. (Previously presented)** The method as in claim 215, wherein said recipient computer  
16 is a user system that is directly accessible by the recipient, said user system including electronic  
17 mail processing software and being capable of receiving e-mail.

18  
19 **218. (Currently amended)** The method as in claim 260, wherein said acquired recipient  
20 data is ~~further~~ related to a biometric imprint, alphanumeric text identification, password  
21 identification, a computer generated user code, or a combination thereof.

22  
23 **219. (Previously presented)** The method as in claim 260, wherein said acquired recipient  
24 data comprises identity information that identifies an individual.

1 **220. (Previously presented)** The method as in claim 260 further comprising means for  
2 recognizing biometric attributes of an individual.

3  
4 **221. (Previously presented)** The method as in claim 260, wherein said acquired recipient  
5 data comprises information that identifies a business.

6  
7 **222. (Previously presented)** The method as in claim 260, wherein said acquired recipient  
8 data comprises information that identifies an organization.

9  
10 **223. (Previously presented)** The method as in claim 260, wherein said acquired recipient  
11 data comprises a computer generated user code.

12  
13 **224. (Currently amended)** The method as in claim 260 further including the step of  
14 including in said confirmation of receipt notice sending access event data of ~~attendant~~ conditions  
15 attendant of said access event.

16  
17 **225. (Previously presented)** The method as in claim 260, wherein said recipient is an  
18 individual.

19  
20 **226. (Previously presented)** The method as in claim 260, wherein said recipient is a  
21 business.

22  
23 **227. (Previously presented)** The method as in claim 260, wherein said recipient is an  
24 organization.

25  
26  
27

1 228. (Currently amended) The method as in claim 260, wherein said ~~confirmation of~~  
2 receipt notice sent recipient data is used to verify proper delivery of legal documents.

3  
4 229. (Currently amended) The method as in claim 260, wherein said ~~confirmation of receipt~~  
5 notice sent recipient data is used to verify proper delivery of confidential documents.

6  
7 230. Canceled.

8  
9 231. (Previously presented) The method as in claim 260, wherein said recipient data is  
10 acquired as a requisite condition for permitting access to said delivered e-mail.

11  
12 232. (Previously presented) The method as in claim 260, wherein said recipient data is  
13 acquired as a requisite condition for permitting access to said recipient e-mail address.

14  
15 233. (Previously presented) The method as in claim 260, wherein said recipient data is  
16 acquired as a requisite condition for operating a remote user computer, said remote user computer  
17 being operable to gain access to said recipient e-mail address.

18  
19 234. (Previously presented) The method as in claim 260, wherein said recipient data is  
20 comprised of alphanumeric text, said alphanumeric text being associated with the at least one  
21 biometric attribute of said recipient.

22  
23 235. (Previously presented) The method as recited in claim 256 wherein the step of  
24 sending at least some of the discovered identifying data for confirming proper delivery of said e-  
25 mail includes the steps of:

1 a) generating a confirmation of receipt notice wherein the acquired identifying data is  
2 included with said confirmation of receipt notice; and

3 b) sending said confirmation of receipt notice wherein the acquired identifying data  
4 contained with said confirmation of receipt notice can be compared to information associated with  
5 said intended recipient in order to verify whether the e-mail was accessed by the intended recipient.

6  
7 **236. (Previously presented)** A method for verifying whether an e-mail sent by a sending  
8 party was accessed by an intended recipient, said method comprising:

9 a) transmitting an e-mail from a sender computer to an intended recipient, the sender  
10 computer being connected to a communications network;

11 b) delivering said e-mail to a recipient e-mail address;

12 c) detecting an access event, and prompting the party associated with said access event to  
13 input recipient data prior to allowing the requested access, said recipient data including identifying  
14 data related to the party associated with said requested access; and

15 d) sending recipient data for confirming proper delivery of said e-mail.

16  
17 **237. (Currently amended)** The method recited by claim 264 wherein the step of sending  
18 data that identifies said recipient for confirming proper delivery of said e-mail includes the steps of:

19 a) generating a confirmation of receipt notice wherein the ~~acquired-recipient data~~ that  
20 identifies the recipient is included ~~in~~ with said confirmation of receipt notice; and

21 b) sending said confirmation of receipt notice, wherein the ~~acquired-recipient data~~ that  
22 identifies the recipient that is included ~~contained-in~~ with said confirmation of receipt notice can be  
23 compared to delivery information associated with said intended recipient in order to verify whether  
24 the email was accessed by the intended recipient.

1 **238. (Previously presented)** The method as in claim 264, wherein said data that identifies  
2 said recipient is related to a biometric imprint, alphanumeric text identification, password  
3 identification, a computer generated user code, or a combination thereof.

4  
5 **239. (Currently amended)** The method as in claim 264, wherein the data that identifies  
6 said recipient is comprised of alphanumeric text, said alphanumeric text being associated with the at  
7 least one biometric attribute of said recipient.

8  
9 **240. (Previously presented)** The method as in claim 264 further including the step of  
10 recognizing biometric attributes of an individual.

11  
12 **241. (Previously presented)** The method as in claim 264, wherein said data that identifies  
13 said recipient comprises identity information that identifies an individual.

14  
15 **242. (Previously presented)** The method as in claim 264, wherein said data that identifies  
16 said recipient comprises information that identifies a business.

17  
18 **243. (Previously presented)** The method as in claim 264, wherein said data that identifies  
19 said recipient comprises information that identifies an organization.

20  
21 **244. (Previously presented)** A system for verifying whether e-mail sent by a sending party  
22 was accessed by an intended recipient, said system comprising:

23 a) a sender computer connected to a communications network and from which an email is  
24 transmitted;

1           b) a recipient computer connected to said communications network, said recipient computer  
2 capable of receiving said transmitted e-mail and further having a data storage for storing said  
3 received e-mail;

4           c) a data file stored on a computer associated with e-mail retrieval , said stored data file  
5 associated with a particular recipient e-mail address and identifying a party associated with said  
6 particular e-mail address;

7           d) software capable of detecting an access event, wherein, upon detecting said access  
8 event, said software discovers the stored data file that is associated with the particular e-mail  
9 address to which said e-mail was delivered; and

10          e) means for sending the discovered data file for confirming proper delivery of said e-mail.

11  
12 **245. (Previously presented)**       The system as in claim 275, wherein said access event  
13 comprises access of a delivered e-mail.

14  
15 **246. (Previously presented)**       The system as in claim 275, wherein said access event  
16 comprises access of an e-mail account associated with the e-mail address to which said e-mail was  
17 delivered.

18  
19 **247. (Previously presented)**       The system as in claim 275, wherein said access event  
20 comprises activation of the e-mail processing software associated with the e-mail address to which  
21 said e-mail was delivered.

22  
23 **248. (Previously presented)**       A system for verifying whether e-mail sent by a sending party  
24 was accessed by an intended recipient, said system comprising:

25           a) a sender computer connected to a communications network and from which an e-  
26 mail is transmitted;

1           b) a recipient computer connected to said communications network, said recipient  
2 computer capable of receiving said transmitted e-mail and further having data storage means for  
3 storing said received e-mail;

4           c) software capable of detecting an access event, wherein, upon detecting said access  
5 event, said software prompts the party associated with said access event to input recipient data prior  
6 to allowing the requested access, said recipient data comprising identifying data related to the party  
7 associated with said requested access; and

8           d) means for sending recipient data for confirming proper delivery of said e-mail.

9  
10 **249. (Previously presented)** The system as in claim 248, wherein said access event comprises  
11 access of a delivered e-mail.

12  
13 **250. (Previously presented)** The system as in claim 248, wherein said access event  
14 comprises access of an e-mail account associated with the e-mail address to which said e-mail was  
15 delivered.

16  
17 **251. (Previously presented)** The system as in claim 248, wherein said access event  
18 comprises activation of e-mail processing software associated with the e-mail address to which said  
19 e-mail was delivered.

20  
21 **252. (Previously presented)** A system for verifying whether e-mail sent by a sending party  
22 was accessed by an intended recipient, said system comprising:

23           a) a sender computer connected to a communications network and from which an e-mail is  
24 transmitted;

25           b) a recipient computer connected to said communications network, said recipient  
26 computer being capable of receiving said transmitted e-mail and further having data storage means  
27



1 for storing said received e-mail;

2 c) biometric identification means for recognizing biometric attributes of an individual;

3 d) software capable of detecting an access event and identifying an individual through  
4 utilization of inputted biometric attributes of said individual; and

5 e) means for sending data that identifies said individual for confirming proper delivery of  
6 said e-mail.

7  
8 **253. (Previously presented)** The system as in claim 252, wherein said access event  
9 comprises access of a delivered e-mail.

10  
11 **254. (Previously presented)** The system as in claim 252, wherein said access event  
12 comprises access of an e-mail account associated with the e-mail address to which said e-mail was  
13 delivered.

14  
15 **255. (Previously presented)** The system as in claim 252, wherein said access event comprises  
16 activation of e-mail processing software associated with the e-mail address to which said e-mail was  
17 delivered.

18  
19 **256. (Previously presented)** A method for verifying whether an e-mail sent by a sending  
20 party was accessed by an intended recipient, said method comprising:

21 a) storing recipient data in a data file, said data file containing identifying data that  
22 identifies a recipient of e-mail and being associated with said recipient's e-mail address;

23 b) transmitting an e-mail from a sender computer to an intended recipient, the sender  
24 computer being connected to a communications network;

25 c) delivering said e-mail to an e-mail address;

26 d) detecting an access event, and discovering the stored data file that is associated with the  
27

1 e-mail address to which said e-mail was delivered; and

2 e) sending at least some of the identifying data contained in said discovered data file for  
3 confirming proper delivery of said e-mail.

4  
5 **257. (Previously presented)** A method for verifying whether an e-mail sent by a sending party  
6 was accessed by an intended recipient, said method comprising:

7 a) storing recipient data in a data file, said data file containing identifying data that  
8 identifies a recipient of e-mail and being associated with said recipient's e-mail address;

9 b) transmitting an e-mail from a sender computer to an intended recipient, the sender  
10 computer being connected to a communications network;

11 c) delivering said e-mail to an e-mail address;

12 d) detecting an access event, and discovering the stored data file that is associated with the  
13 e-mail address to which said e-mail was delivered; and

14 e) sending the discovered data file for confirming proper delivery of said e-mail.

15  
16 **258. (Previously presented)** A method for verifying whether an e-mail sent by a sending  
17 party was accessed by an intended recipient, said method comprising:

18 a) transmitting an e-mail from a sender computer to an intended recipient, the sender  
19 computer being connected to a communications network;

20 b) delivering said e-mail to an e-mail address;

21 c) detecting an access event, and prompting the party that requested said access to input  
22 recipient data prior to allowing the requested access, said recipient data including identifying data  
23 that is associated with the party that requested said access; and

24 d) sending recipient data for confirming proper delivery of said e-mail.

25  
26 **259. (Previously presented)** The method recited by claim 236 wherein said step of sending

27

1 recipient data for confirming proper delivery of said e-mail includes the steps of:

2 a) generating a confirmation of receipt notice wherein the inputted recipient data is included  
3 with said confirmation of receipt notice; and

4 b) sending said confirmation of receipt notice, wherein the inputted recipient data included  
5 with said confirmation of receipt notice can be compared to information associated with said  
6 intended recipient in order to verify whether the e-mail was accessed by the intended recipient.

7  
8 **260. (Previously presented)** A method for verifying whether e-mail sent by a sending party  
9 was accessed by an intended recipient, said method comprising:

10 a) transmitting an e-mail from a sender computer to an intended recipient, the sender  
11 computer being connected to a communications network;

12 b) delivering said e-mail to a recipient e-mail address;

13 c) detecting an access event;

14 d) acquiring recipient data that is related to biometric identification of the recipient; and

15 e) sending recipient data for confirming proper delivery of said e-mail.

16  
17 **261. (Previously presented)** The method as recited in claim 260 wherein said recipient data is  
18 acquired prior to said access event.

19  
20 **262. (Previously presented)** The method as recited in claim 260 wherein said recipient data is  
21 acquired after said access event.

22  
23 **263. (Previously presented)** The method as recited in claim 260 wherein said recipient data is  
24 sent to an e-mail address.

25  
26 **264. (Previously presented)** A method for verifying whether e-mail sent by a sending party was  
27

1 accessed by an intended recipient, said method comprising:

- 2 a) transmitting an e-mail from a sender computer to an intended recipient, the sender  
3 computer being connected to a communications network;  
4 b) delivering said e-mail to an e-mail address;  
5 c) identifying a recipient utilizing biometric identification;  
6 d) detecting an access event; and  
7 e) sending data that identifies said recipient for confirming proper delivery of said e-mail.

8  
9 **265. (Previously presented)** The method as recited in claim 264 wherein said recipient is  
10 identified prior to said access event.

11  
12 **266. (Previously presented)** The method as recited in claim 264 wherein said recipient is  
13 identified after said access event.

14  
15 **267. (Previously presented)** The method as recited in claim 264 wherein said data that identifies  
16 said recipient is sent to an e-mail address.

17  
18 **268. (Previously presented)** A method for verifying whether e-mail sent by a sending party was  
19 accessed by an intended recipient, said method comprising:

- 20 a) transmitting an e-mail from a sender computer to an intended recipient, the sender  
21 computer being connected to a communications network;  
22 b) delivering said e-mail to an e-mail address;  
23 c) identifying a recipient in association with biometric identification;  
24 d) detecting an access event; and  
25 e) sending data that identifies said recipient for confirming proper delivery of said e-mail.

1 **269. (Previously presented)** The method as in claim 268 wherein said recipient is identified prior  
2 to said access event.

3  
4 **270. (Previously presented)** The method as in claim 268 wherein said recipient is identified after  
5 said access event.

6  
7 **271. (Previously presented)** The method as in claim 268 wherein said data that identifies said  
8 recipient is sent to an e-mail address.

9  
10 **272. (Currently amended)** A method for verifying whether an e-mail sent by a sending party was  
11 accessed by an intended recipient, said method comprising:

12 a) storing recipient data on a storage element of a computer that is used by a recipient of e-  
13 mail to access e-mail, said recipient data including identifying data that is associated with a  
14 recipient of e-mail;

15 b) transmitting an e-mail from a sender computer to an intended recipient, the sender  
16 computer being connected to a communications network;

17 c) delivering said e-mail to ~~an~~ a recipient e-mail address;

18 d) detecting an access event and discovering at least part of said stored recipient data that is  
19 associated with said recipient;

20 e) sending at least part of said discovered recipient data for confirming proper delivery of  
21 said e-mail.

22  
23 **273. (Previously presented)** The method recited in claim 272 wherein said recipient of e-mail is  
24 an actual recipient of said e-mail.

1 **274. (Previously presented)** The method recited in claim 244 wherein said recipient of e-mail is  
2 an actual recipient of said e-mail.

3  
4 **275. (Previously presented)** A system for verifying whether e-mail sent by a sending party was  
5 accessed by an intended recipient, said system comprising:

6 a) a sender computer connected to a communications network and from which an e-mail is  
7 transmitted;

8 b) a recipient computer connected to said communications network, said recipient computer  
9 capable of receiving said transmitted e-mail and further having a data storage for storing said  
10 received e-mail;

11 c) a data file stored on a computer, said stored data file containing identifying data  
12 pertaining to a party and associated with said party's e-mail address;

13 d) software capable of detecting an access event, wherein, upon detecting said access  
14 event, said software discovers identifying data contained in said stored data file that is associated  
15 with the e-mail address to which said e-mail was delivered; and

16 e) means for sending identifying data for confirming proper delivery of said e-mail.

17  
18 **276. (Previously presented)** The system as recited in claim 275 wherein said recipient of e-mail  
19 is an actual recipient of said e-mail.

20  
21 **277. (Previously presented)** The system as recited in claim 275 wherein said identifying data for  
22 confirming proper delivery of said e-mail is sent to an e-mail address.

23  
24 **278. (Previously presented)** A system for verifying whether e-mail sent by a sending party  
25 was accessed by an intended recipient, said system comprising:

1 a) a sender computer connected to a communications network and from which an e-mail is  
2 transmitted;

3 b) a recipient computer connected to said communications network, said recipient computer  
4 capable of receiving said transmitted e-mail and further having a data storage for storing said  
5 received e-mail;

6 c) recipient data stored on the data storage of a computer that is used by a recipient of e-  
7 mail to access e-mail, said recipient data including identifying data that is associated with a  
8 recipient of e-mail;

9 d) software capable of detecting an access event, wherein, upon detecting said access  
10 event, said software discovers at least part of said stored recipient data that is associated with said  
11 recipient; and

12 e) means for sending at least part of said discovered recipient data for confirming proper  
13 delivery of said e-mail.

14  
15 **279. Canceled.**

16  
17 **280. (Previously presented)** The system as recited in claim 278, wherein said recipient data is  
18 contained in a  
19 data file, said data file being stored on said storage of said computer.

20  
21 **281. (Previously presented)** The system as recited in claim 278, wherein recipient data pertaining  
22 to said recipient of e-mail is stored on said storage prior to said access event.

23  
24 **282. (Previously presented)** The system as recited in claim 278, wherein said at least part of said  
25 discovered recipient data for confirming proper delivery of said e-mail is sent to an e-mail address.

1 **283. (Previously presented)** The system as recited in claim 278, wherein said access event  
2 comprises access of a delivered e-mail.

3  
4 **284. (Previously presented)** The system as recited in claim 278, wherein said access event  
5 comprises access of an e-mail account associated with the e-mail address to which said e-mail was  
6 delivered.

7  
8 **285. (Previously presented)** The system as recited in claim 278, wherein said access event  
9 comprises activation of an e-mail processing software associated with the e-mail address to which  
10 said e-mail was delivered.

11  
12 **286. (Previously presented)** The method as recited in claim 257 wherein the step of sending the  
13 discovered data file for confirming proper delivery of said e-mail includes the steps of:

14 a) generating a confirmation of receipt notice wherein the discovered data file is included  
15 with said confirmation of receipt notice; and

16 b) sending said confirmation of receipt notice, wherein the identifying data in the  
17 discovered data file that is included with said confirmation of receipt notice can be compared to  
18 information associated with said intended recipient in order to verify whether the email was  
19 accessed by the intended recipient.

20  
21 **287. (Previously presented)** The method as recited in claim 272 wherein the step of sending at  
22 least part of said discovered recipient data for confirming proper delivery of said e-mail includes the  
23 steps of:

24 a) generating a confirmation of receipt notice wherein the discovered recipient data is  
25 included with said confirmation of receipt notice; and



1           b) sending said confirmation of receipt notice, wherein the discovered recipient data  
2 included with said confirmation of receipt notice can be compared to information associated with  
3 said intended recipient in order to verify whether the email was accessed by the intended recipient.  
4

5 **288. (Previously presented)** The method as in claim 287, wherein said confirmation of receipt  
6 notice is sent to an e-mail address.  
7

8 **289. (Previously presented)** The method as in claim 272, wherein said access event  
9 comprises access of said e-mail that was delivered to said recipient e-mail address.  
10

11 **290. (Previously presented)** The method as in claim 272, wherein said access event comprises  
12 access of an e-mail account associated with said recipient e-mail address.  
13

14 **291. (Previously presented)** The method as in claim 272, wherein said access event comprises  
15 activation of an e-mail processing software associated with said recipient e-mail address.  
16

17 **292. (Previously presented)** The method as in claim 272, wherein the step of transmitting  
18 an e-mail from a sender computer includes attaching an executable attachment file in conjunction  
19 with the e-mail file, the executable attachment file having a first module for discovering the stored  
20 recipient data that is associated with said recipient, and wherein the step of detecting an access  
21 event includes the step of executing the first module of the executable attachment.  
22

23 **293. (Previously presented)** The method as in claim 292, wherein the executable  
24 attachment file has a second module transmitted and delivered therewith, the second module for  
25 detecting the access event, and further comprising the step of:

26           automatically executing the second module upon delivery of the attachment file to said  
27

1 recipient e-mail address.

2

3 **294. (Previously presented)** The method as in claim 272, wherein said recipient e-mail  
4 address is associated with a recipient computer.

5

6 **295. (Previously presented)** The method as in claim 294, wherein said recipient computer  
7 is a server of a service provider.

8

9 **296. (Previously presented)** The method as in claim 294, wherein said recipient computer is a  
10 user system that is directly accessible by a recipient, said user system including electronic mail  
11 processing software.

12

13 **297. (Previously presented)** The method as in claim 272, wherein a remote user computer  
14 may be used to gain remote access to said recipient e-mail address.

15

16 **298. (Previously presented)** The method as in claim 272, wherein said computer on which said  
17 recipient data is stored is a recipient computer.

18

19 **299. (Previously presented)** The method as in claim 272, wherein said computer on which said  
20 recipient data is stored is a remote user computer.

21

22 **300. (Previously presented)** The method as in claim 272, wherein said recipient data is contained  
23 in a data file, said data file being stored on said storage element of said computer.

24

25 **301. (Previously presented)** The method as in claim 272, wherein said storage element comprises  
26 of a hard disk drive.

27

1  
2 **302. (Previously presented)** The method as in claim 272, wherein said storage element comprises  
3 of a memory module.

4  
5 **303. (Previously presented)** The method as in claim 272, wherein recipient data pertaining to said  
6 recipient of e-mail is stored on said storage element prior to said access event.

7  
8 **304. (Previously presented)** The method as in claim 272, wherein said stored recipient data  
9 pertains to alphanumeric text identification, biometric identification, password identification, a  
10 computer generated user code, or a combination thereof.

11  
12 **305. (Currently amended)** The method as in claim 272, wherein said stored recipient data  
13 comprises, ~~at least~~, identity information that identifies an individual.

14  
15 **306. (Previously presented)** The method as in claim 305, wherein said identity information  
16 pertains to biometric identification.

17  
18 **307. (Currently amended)** The method as in claim 306 further comprising ~~means for the~~  
19 step of recognizing biometric attributes of an individual.

20  
21 **308. (Previously presented)** The method as in claim 305, wherein said identity information  
22 includes alphanumeric text identification data .

23  
24 **309. (Currently amended)** The method as in claim 272, wherein said stored recipient  
25 data includes, ~~at least~~, information that identifies a business.

1 **310. (Currently amended)** The method as in claim 272, wherein said stored data  
2 includes, ~~at least~~, information that identifies an organization.

3  
4 **311. (Currently amended)** The method as in claim 272, wherein said stored recipient data  
5 includes, ~~at least~~, a computer generated user code.

6  
7 **312. (Previously presented)** The method as in claim 272 further including the step of  
8 sending access event data of attendant conditions of said access event.

9  
10 **313. (Previously presented)** The method as in claim 272, wherein said recipient is an  
11 individual.

12  
13 **314. (Previously presented)** The method as in claim 272, wherein said recipient is a business.

14  
15 **315. (Previously presented)** The method as in claim 272, wherein said recipient is an  
16 organization.

17  
18 **316. (Previously presented)** The method as in claim 272, wherein said sent recipient data  
19 is used to verify proper delivery of legal documents.

20  
21 **317. (Previously presented)** The method as in claim 272, wherein said sent recipient data  
22 is used to verify proper delivery of confidential documents.

23  
24 **318. (Previously presented)** The method as in claim 272, wherein said at least part of the  
25 discovered recipient data for confirming proper delivery of said e-mail is sent to an e-mail address.

1 **319. (Previously presented)** The method as recited in claim 256, wherein said identifying data  
2 for confirming proper delivery of said e-mail is sent to an e-mail address.

3  
4 **320. (Previously presented)** The method as recited in claim 256, wherein said data file is stored  
5 on a computer associated with e-mail retrieval.

6  
7 **321. (Previously presented)** The method as in claim 235, wherein said confirmation of receipt  
8 notice is sent to an e-mail address.

9  
10 **322. (Previously presented)** The method as in claim 256, wherein said identifying data  
11 contained in said stored data file pertains to alphanumeric text identification, biometric  
12 identification, password identification, a computer generated user code, or a combination thereof.

13  
14 **323. (Previously presented)** The method as in claim 257, wherein said data file is sent to an e-  
15 mail address.

16  
17 **324. (Previously presented)** The method as in claim 257, wherein said data file is stored on a  
18 computer associated with e-mail retrieval.

19  
20 **325. (Previously presented)** The method as in claim 286, wherein said confirmation of receipt  
21 notice is sent to an e-mail address.

22  
23 **326. (Previously presented)** The method as in claim 257, wherein said identifying data  
24 contained in said stored data file pertains to alphanumeric text identification, biometric  
25 identification, password identification, a computer generated user code, or a combination thereof.

1 **327. (Previously presented)** The method as in claim 236, wherein said recipient data for  
2 confirming proper delivery of said e-mail is sent to an e-mail address.

3  
4 **328. (Previously presented)** The method as in claim 236, wherein a remote user computer may  
5 be used to gain remote access to said recipient e-mail address.

6  
7 **329. (Previously presented)** The method as in claim 236 wherein the party that is associated  
8 with said access event is an individual.

9  
10 **330. (Previously presented)** The method as in claim 236 wherein the party that is associated  
11 with said access event is a business.

12  
13 **331. (Previously presented)** The method as in claim 236 wherein the party that is associated  
14 with said access event is an organization.

15  
16 **332. (Previously presented)** The method as in claim 258 wherein said recipient data for  
17 confirming proper delivery of said e-mail is sent to an e-mail address.

18  
19 **333. (Previously presented)** The method as in claim 184, wherein said confirmation of receipt  
20 notice is sent to an e-mail address.

21  
22 **334. (Previously presented)** The method as in claim 258, wherein said inputted recipient data  
23 pertains to alphanumeric text identification, biometric identification, password identification, a  
24 computer generated user code, or a combination thereof.

25  
26 **335. (Previously presented)** The method as in claim 208, wherein said confirmation of receipt  
27

1 notice is sent to an e-mail address.

2  
3  
4 **336. (Previously presented)** The method as in claim 260, wherein a remote user computer may  
5 be used to gain remote access to said recipient e-mail address.

6  
7 **337. (Previously presented)** The method as in claim 219, wherein said identity information  
8 includes alphanumeric text identification.

9  
10 **338. (Previously presented)** The method as in claim 237, wherein said confirmation of receipt  
11 notice is sent to an e-mail address.

12  
13 **339. (Previously presented)** The method as in claim 268 , wherein said data that identifies  
14 said recipient is related to a biometric imprint, alphanumeric text identification, password  
15 identification, a computer generated user code, or a combination thereof.

16  
17 **340. (Currently amended)** The method as in claim 268 further comprising means for the  
18 step of recognizing biometric attributes of an individual.

19  
20 **341. (Previously presented)** A method for verifying whether an e-mail sent by a sending party  
21 was accessed by an intended recipient, said method comprising:

22 a) storing recipient data on a storage element of a computer that is used to access e-mail,  
23 said recipient data including identifying data that is associated with a recipient of e-mail;

24 b) transmitting an e-mail from a sender computer to an intended recipient, the sender  
25 computer being connected to a communications network;

26 c) delivering said e-mail to an e-mail address;

27

1 d) detecting an access event and discovering at least part of said stored recipient data that is  
2 associated with said recipient;

3 e) sending at least part of said discovered recipient data for confirming proper delivery of  
4 said e-mail.

5  
6 **342. (Previously presented)** The system as in claim 244, wherein said discovered data file for  
7 confirming proper delivery of said e-mail is sent to an e-mail address.

8  
9 **343. (Previously presented)** The system as in claim 244, wherein said access event comprises  
10 access of a delivered e-mail.

11  
12 **344. (Previously presented)** The system as in claim 244, wherein said access event comprises  
13 access of an e-mail account associated with the e-mail address to which said e-mail was delivered.

14  
15 **345. (Previously presented)** The system as in claim 244, wherein said access event comprises  
16 activation of an e-mail processing software associated with the e-mail address to which said e-mail  
17 was delivered.

18  
19 **346. (Previously presented)** The system as in claim 248, wherein said recipient data for  
20 confirming proper delivery of said e-mail is sent to an e-mail address.

21  
22  
23 **347. (Previously presented)** The system as in claim 252, wherein said individual is identified  
24 prior to said access event.

25  
26 **348. (Previously presented)** The system as in claim 252, wherein said individual is identified



1 after said access event.

2

3 349. (Previously presented) The system as in claim 252, wherein said data that identifies said  
4 individual for confirming proper delivery of said e-mail is sent to an e-mail address.

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27